Applying a Reference Document of the Organizational Structure for Cyber Security Operation

TAKEI Shigenori

Abstract

This article presents applying a reference document of the organizational structure of the cyber security operations for the Olympic and Paralympic Games Tokyo 2020, which was commissioned to perform by NTT Group. What issues were found in actual operational situations after the establishment of the system? Based on the experience of the actual operations of the Olympic and Paralympic Games Tokyo 2020 and the differences between the assumptions in the reference document and the actual operations of the Olympic and Paralympic Games Tokyo 2020, this article discusses points to be noted in future large-scale events.

Keywords : Tokyo 2020 Games, Security operation, SOC, CSIRT

1. Introduction

The security monitoring and operation of the back-office network (Back Office Network) used by the members of the Tokyo Organising Committee of the Olympic and Paralympic Games of the Olympic and Paralympic Games Tokyo 2020 (hereinafter referred to as "Tokyo 2020 Games") was conducted by the Tokyo 2020 Organising Committee and the NTT Group which was entrusted with the security operation. The "Textbook for Security Response Organizations, Version 2.1" (Reference (1)) published by the Information Security Operation providers Group Japan (ISOG-J) was applied as a reference document for building the security operation team. I am one of the authors of Reference (1). This article discusses the operational issues as the author of Reference (1) during the actual operation in NTT-SOC from April to the end of September 2021.

2. Organizational Structure with Reference Documents

Reference (1) is a document in Japan that shows the overview of security activities in the organization, including the SOC (Security Operation Centre) and CSIRT (Computer Security Incident Response Team). It comprehensively describes the functions, roles, and operations to be performed in the organization. The contents of Reference (1) were subsequently contributed to the International Telecommunication Union Telecommunication Standardization Sector (hereinafter referred to as ITU-T) and incorporated into ITU-T Recommendation X.1060 (hereinafter referred to as Reference (2)) in the field of security management.

Preparations for security operations for the Tokyo 2020 Games began around 2016, and NTT-SOC was responsible for the formulation and operation of the following tasks out of 10 categories of tasks, referring to Reference (1).

TAKEI Shigenori
Secure System Business Department, NTT TechnoCross Corporation
E-mail takei.shigenori@ntt-tx.co.jp
The Journal of The Institute of Electronics, Information and Communication Engineers, Vol.105, No.8, Supplement, pp.291-293, August 2022

B. Real-time analysis
D. Incident response
E. Checking and evaluation
F. Collection, analysis and evaluation of threat intelligence
G. Development and maintenance of security operation platforms

NTT-SOC implemented SOC and CSIRT functions in cooperation with the organising committee. The author worked in the "Incident Response Senior Expert"(IRSE) team in an advisory position supporting the SOC and CSIRT teams.

3. Operational considerations during the operation period

The organizational structure was established during the preliminary preparation period, and the members assigned ahead of the others were performing their duties and developing procedures for operations. In June 2021, other members were assigned and increased the maturity of operations, at last, Tokyo 2020 Games were held. The operations were well-organized, and the workflow and procedures had been prepared in the organizational structure. But there were three major operational issues during the operation period.

Issue (1) : Due to the siloed organization and teams, necessary collaboration was not sufficient.

Although NTT-SOC implemented the functions described above, there were some difficulty points to handle. One was to deal with unanticipated or newly added tasks and products, and the other was to develop new team collaboration.

On the other hand, the IRSE team was able to support collaboration and cover a wide range of work because of its broad scope. Not only that, but each team member also collaborated with the organising committee at the field to implement a series of workflows as one team. Nevertheless, these efforts were largely due to the efforts of human resources onsite, and the system for organizational solutions will be needed in the future.

Issue (2) : Because of the time-limited organization, there was a tendency for the improvement cycle to optimize the entire organization and operations to be difficult to implement.

Related to issue (1) above, the scope of improvement of the organization and operations is closed within the team due to the time limit of the organization. As a result, the entire organization had not been optimized through improvement. At the management process in Reference (1) and (2), it is assumed that not only improvements at the field level but also continuous improvements at the organizational level will be continued. In this case, the organizational structure had already been decided, and it was not possible to make improvements such as reorganizing the organization to match the actual situation of the business during the preparation and holding periods. On the other hand, since preparations are made over a period of several years, it is necessary to assume that the organizational structure will change from the initial assumption, and that the allocation of resources can be changed by organizing teams and reviewing operations, even if the organizational structure cannot be changed.

Issue (3) : The understanding of the characteristics of security-related operations was not fully unified as a preliminary image of the work to be performed by the personnel.

Experts with various backgrounds and skills were gathered as members. Experts with experience in SOC operations and the other experts with experience in common system and network operations got training in SOC operations before being assigned to the team. In common system and network operations, the causes of possible failures are sudden and unexpected, such as "disasters" and "failures," and most of the response procedures follow procedure manuals. On the other hand, security operations are often caused by "human factors" and require continuous monitoring of changing attacks. Therefore, it is not always possible to analyze and respond to attacks using only assumed procedures. It is necessary to be constantly aware of new methods and responses to new attacks, and to keep updating work flows and procedures. The work flows and procedures are almost same in the operations, such as monitoring and responding to any anomalies. However, it is necessary to conduct training that includes case studies that make it easier to recognize the differences in security thinking and to improve the ability to respond to and deal with security issues by daily awareness of them after being assigned to a SOC.

If we consider similar large-scale events in the future, we can refer to the new guidelines and documents

related to Reference (1), Reference (2) and METI Cyber Security Management Guidelines[3] can be used as references.

An entity that can provide comprehensive support for cybersecurity of the business as a whole is needed.

Reference (2) also defines a framework for continuous evaluation and improvement. If it takes several years including preparation, it is necessary to have the organization that can review and improve according to the changes, based on the assumption that the surrounding conditions will certainly change.

4. In closing

The organization structure and operations were designed based on Reference (1), and a comprehensive definition and assignment of operations were established. On the other hand, the operational aspects were not the best, and the good and bad points became the lessons, examples and references for the future (so-called "legacy"). The good points can be used as a reference for future work by the members involved in SOC and CSIRT operations. As for the bad points that each member felt the need to improve, they can refer to them when they return to their work. These will lead to the next large-scale event and daily operations.

Finally, I would like to thank the team members who worked positively in this difficult situation, as well as the members of the organising committee for their cooperation and support. I would also like to thank the organising committee for providing me with the opportunity to utilize and discuss the documents I was involved within a large-scale event, even it happened consequently. We hope that this document will serve as a reference for those who are involved in the security of large-scale events that take several years to prepare.

References

(1) Textbook for security response organizations, Version 2.1, security operations chaos working group (WG6) of the information security operation providers group Japan, 2018.
Available at : https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

(2) "X.1060 : Framework for the creation and operation of a cyber defence centre," ITU-T.2021.
https://www.itu.int/rec/T-REC-X.1060-202106-I

(3) Ministry of economy, trade and industry, cybersecurity management guidelines appendix F : guidance for establishing cyber security system and securing human resources, version 1.1, 2021.
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

(Received February 28, 2022, last received March 15, 2022)

TAKEI Shigenori

TAKEI Shigenori graduated from Shinshu University in 1998 with a bachelor's degree in engineering and information technology, and completed a master's degree at Shinshu University in 2000. He joined NTT Software Corporation (now NTT TechnoCross Corporation) in the same year, where he was engaged in security consulting. He is a principal grade of NTT Group security certificate, a CISSP, a Registered Information Security Specialist, Vice President and the leader of WG6 of the Information Security Operation providers Group Japan. The editor of ITU-T SG17 WP3 Q3 X.1060.